What is Claimed is:

1. A method of ensuring the security of patient's data from medical tests conducted by a third-party, the method comprising:

providing the patient with a medical data card containing a unique patient identification number;

taking a specimen from the patient for conducting the medical test;

generating a first medical test request containing the unique patient identification number using the patient's medical data card, and

transmitting the specimen and the first medical test request to a third party data provider that generates a second medical test request devoid of accessible patient identification information using the first medical test request and transmits the specimen and second medical test to a third party laboratory and receives the results from the laboratory, and reports the results on a test results card that can only be read in conjunction with the patient's medical data card.

2. The method according to claim 1 further comprising reading the test results on the test results card using the patient's medical data card.

3. The method according to claim 1 wherein the patient's medical data card includes a memory, and further comprising the step of storing the test results in the memory on the patient's medical data card.

4. The method according to claim 1 wherein the patient identification number is not readable from the patient's medical data card without a PIN, and wherein the step of generating the first medical test request includes the patient supplying the PIN.

5. The method according to claim 2 wherein the test results are not readable with the medical data card without a PIN, and wherein the step of reading the test results on the test results card includes the patient supplying the PIN.

6. A method of ensuring the security of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the method comprising:

issuing the patient a medical data card containing a unique patient identification number;

receiving from the medical provider a first request for a medical test generated using the patient's medical data card, and a patient specimen for use in conducting the test;

generating a second request for a medical test using the first request for a medical test, the second request for a medical test being devoid of publicly accessible information about the identity of the patient;

forwarding the second request for a medical test and the specimen to a third party laboratory for conducting the test, and receiving the results of the test from the laboratory; and

providing the tests results to the medical provider in a form that can only be read in conjunction with the patient's medical data card.

7. The method of claim 6, wherein the tests results are on a tests results card in computer readable form and the method further comprises providing the medical provider with a reader adapted for reading the tests results.

8. A medical data card for use in a system for ensuring the security of a patient's data from medical tests conducted for a medical provider by a third-party laboratory, the medical data card including a unique patient ID code, a public key encryption private key, and a public key encryption public key, and a data storage element.

9. The medical data card of claim 8, wherein the data storage element is adapted for storing data for at least one test, including for each test: the type of test, a unique identification code for the test, and the results of the test.

10. A test request card for use in a system for ensuring the security of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the test request card including encrypted information identifying the patient, the test type, an identification of the medical provider, a unique patient identification number, and a public encryption public code.

11. The test request card according to claim 10, wherein at least some of the information on the card is in bar code form.

12. The test request card according to claim 11, wherein at least some of the information on the card is in magnetic form.

13. A test results card for use in a system for ensuring the securing of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the test results card including encrypted information identifying the patient and the results of the medical tests.

14. The test results card according to claim 13, wherein at least some of the information on the card is in bar code form.

15. The test results card according to claim 13, wherein at least some of the information on the card is in magnetic form.

16. The test results card of claim 13, wherein the results are encrypted.

17. The test results card according to claim 15, further comprising a patient identification code.

18. A method of ensuring the security of patient's data from medical tests conducted for a medical provider by a third-party laboratory, the method comprising:

issuing the patient a medical data card containing a unique patient identification number;

receiving from a medical provider a first request for a medical test generated using the patient's medical data card, and a patient specimen for use in conducting the test;

generating a second request for a medical test using the first request for a medical test, the second request for a medical test having encrypted information identifying the patient but being devoid of publicly accessible information about the identity of the patient, and including a public encryption public code specific to the patient;

forwarding the second request for a medical test and the specimen to a third party laboratory for conducting the test, and receiving the results of the test from the laboratory encrypted using the public encryption public code on the second request for a medical test;

identifying the patient to whom the results pertain, and providing the tests results to the appropriate medical provider in the encrypted form that can only be read in conjunction with the patient's medical data card.

19. A method of ensuring the security of data from patient medical tests conducted for medical providers by third party laboratories, comprising:

providing the patient with a medical data card issued by a secure information provider, having a unique patient identification number (PID), a public key encryption private key (Key 1), and a public key encryption public key (Key 2);

taking a specimen from the patient for conducting the test;

generating a first test request using the patient's medical data card, the first test request including an encrypted identification of the patient and the test; a code identifying the health care provider; the patient identification number (PID); public encryption public key; and an identification of the test type;

forwarding the first test request and the specimen to the secure information provider;

generating a second test request including an encryption of the patient's unique identification number, but otherwise devoid of any indicia that would identify the patient, and an encryption code;

forwarding the second test request and the specimen to the third party laboratory for conducting the medical test and providing the test results in encrypted form using the encryption code on the second test request;

receiving the encrypted test results, identifying the appropriate medical provider from encrypted information included with the test results; and forwarding the encrypted test results to the medical provider with an identification of the patient;

decrypting the test results using the patient's medical data card.